Submission to the Senate Standing Committee on Environment, Communications and the Arts

‘The adequacy of protections for the privacy of Australians online’

By Arved von Brasch

Thank you for the opportunity to make a submission on the crucial issue of privacy.

Privacy
I feel that privacy is a crucially important issue for all people. While the argument is often made that those with nothing to hide have nothing to fear, this is insufficient reason to deny people privacy. An obvious example is going to the toilet. It is something we all must do, yet is something we prefer to do in private. This isn't because we are attempting to hide illegal acts, but simply because it makes most of us uncomfortable to be watched. The same is true for many online (and offline, for that matter) activities. Certainly lack of privacy can generate a chilling effect, and comes dangerously close to policing thought crimes.

There are numerous reasons why any particular individual could desire privacy for online activities. There are still minorities in Australia, which, despite anti-discrimination laws, could face severe personal cost if an individual's minority status were to become public knowledge. It is true that some would use privacy to cloak malicious activities, and that's unfortunate. A balance must be struck, with appropriate judicial checks. The government, however, should always err on trusting its citizens. Trust is a two way street. A government that does not trust its citizens invites its citizens to be mistrustful of it.

Private Companies
The selling of personal information to third parties is a contentious issue. There is certainly no reason why this should be illegal as long as the people involved are told in advance that their information will be sold. The collection of personal information in Australia should be based on the assumption that most people do not wish for their personal information to be sold, rather than the converse. That is, while any company should be free to ask their customers if they may share their details with a third party, this must be an opt-in rather than an opt-out process.

Government Agencies
While collection of personal information is a necessary requirement for government agencies, the government must never build profiles of its citizens. This means that only the information necessary for any particular service should be collected by an agency, and different agencies should be prevented from centralising and merging their databases, even for efficiency reasons. Of course, only trusted government staff who require access to this information, for the purpose of their jobs, should have access to this personal information.

As government services move online, the government must take steps to ensure that personal information cannot be intercepted by an eavesdropping third party. This may prove difficult if people's computers are infected with certain viruses or worms. Education programs about Internet safety should probably be part of school curriculums, especially as the Internet increasingly becomes a crucial utility like electricity and water.

Other Issues
Internet Service Providers should be put into a similar category as the postal service and telephone companies. A warrant should be required before eavesdropping on the traffic between a customer and their ISP is allowed. This means that a data retention policy, such as that being considered by the Attorney-General, should not ever become reality.

Severe punishment should be levied against private companies (or government) if they are found to be negligent in personal information being stolen or being made publicly available. Especially if their security systems are breached by a malicious agent, when those security systems were known to be flawed.